



## Privacy e videosorveglianza in Italia

Chiara Fonio

Università Cattolica – Dpt. di Sociologia

Aprile 2006

Riflettere intorno al binomio “sicurezza – nuove tecnologie” significa anche approfondire il livello legislativo. Sempre di più, infatti, i dispositivi tecnologici sono al centro dei dibattiti dei giuristi i quali sono chiamati a formulare risposte concrete nei confronti di un ambito in continuo divenire come quello dei mezzi elettronici di controllo. Inizieremo perciò a descrivere quali siano le tutele della normativa italiana in merito alla videosorveglianza, per poi soffermarci, in altri interventi, sulle leggi inerenti la biometria, le *smart cards* e le intercettazioni. I provvedimenti legislativi vanno letti alla luce della legge n.675 del 1996 sulla protezione dei dati personali<sup>1</sup> che ha sancito “una pacifica rivoluzione della privacy” (Rodotà, 2005: 46) rendendo i cittadini italiani padroni delle informazioni che li riguardano (*ibidem*), sostituita nel 2003 dal Codice in materia di protezione dei dati personali<sup>2</sup>. L’attenzione nei confronti dei potenziali rischi per la privacy dei dispositivi di videosorveglianza è stata più volte sottolineata dall’ex Garante della Privacy Stefano Rodotà negli anni che vanno dal 1999 al 2004. Ricordiamo che la figura del Garante (<http://www.garanteprivacy.it>) è stata istituita l’anno in cui è entrata in vigore la legge n.675; si tratta di un’autorità indipendente costituita da un organo collegiale formato da quattro componenti eletti dal Parlamento per un periodo di 4 anni.

Considerato che il dibattito pubblico, seppur limitato, è stato stimolato dagli interventi del Garante, ci sembra doveroso soffermarci su questi ultimi che hanno prima preceduto, poi resa concreta la necessità di approdare a un provvedimento legislativo *ad hoc*. Già nel 1999 il Garante definiva la videosorveglianza come “un tema di grande rilievo e interesse per l’opinione pubblica” (newsletter 8-15 marzo 1999), il cui utilizzo deve essere conforme<sup>3</sup> alla legge sulla privacy che definisce dato personale qualsiasi informazione che permette l’identificazione di una persona, compresi i suoni e le immagini. E’ interessante sottolineare la notizia presente nella newsletter riguardante una ricerca svolta in collaborazione con il Dipartimento di Sociologia dell’Università di Roma “La Sapienza” per monitorare le diverse forme di videosorveglianza “valutandone anche l’impatto sociale”. L’approccio nei confronti del tema in questione è perciò impostato fin dalle origini in modo non meramente giuridico ma con una specifica attenzione alle possibili conseguenze sociali. Nei mesi successivi l’attenzione nei confronti della videosorveglianza ha continuato ad animare le comunicazioni dell’Autorità, senza tralasciare la dimensione internazionale nei confronti di un fenomeno che era sempre più in crescita. Si trovano per esempio brevi articoli inerenti alla situazione inglese caratterizzata da alcuni episodi di sorveglianza occulta sul posto di lavoro, o al preoccupante numero di videocamere presenti nei luoghi pubblici in Germania. Nonostante questo dispositivo fosse utilizzato da più di dieci anni in alcuni paesi europei, è solo con gli anni ’90 che le installazioni di telecamere incominciano a essere particolarmente numerose.

In Italia, invece, la richiesta da parte degli enti locali per controllare il territorio e il traffico cittadino tramite videosorveglianza risalgono all’inizio del 2000, come si può dedurre da una delle comunicazioni del Garante (newsletter del 28 febbraio – 5 marzo), nella quale si rende esplicita la necessità per i comuni interessati di adeguare la ripresa

<sup>1</sup> La legge è entrata in vigore l’8 maggio dell’anno successivo.

<sup>2</sup> Decreto legislativo del 30 giugno 2003, n.196.

<sup>3</sup> Ovvero: per quale tipo di funzione o finalità viene realizzata, la sicurezza e la conservazione delle immagini e delle riproduzioni, l’uso appropriato rispetto alla finalità e l’informazione agli interessati.

delle immagini alle norme sulla privacy e di adottare alcune cautele, quali limitare la possibilità di ingrandimento delle immagini e il livello di dettaglio sui tratti somatici. Va comunque aggiunto che le richieste “ufficiali” da parte degli enti locali si inseriscono, come vedremo in seguito, in una situazione in cui l’installazione delle telecamere era già una pratica piuttosto consolidata nel nostro paese. Si insiste inoltre sulle garanzie che devono essere rispettate al fine di tutelare la sfera privata dei cittadini, garanzie già sancite dal regolamento n.318/99 inerente alle misure minime di sicurezza per i dati personali oggetto di trattamento. I cittadini devono sapere se si trovano in prossimità di telecamere attraverso l’affissione di appositi avvisi e deve essere inoltre rispettato il principio di non eccedenza dei dati in relazione agli scopi perseguiti.

Il 2000 segna un passo in avanti importante nell’ambito in questione. Viene infatti svolta dall’Autorità nel periodo compreso tra marzo e maggio un’indagine esplorativa sulla videosorveglianza esterna visibile in 4 città italiane – Milano, Verona, Roma e Napoli- per fornire una valutazione preliminare. Si tratta dell’unica ricerca attualmente disponibile condotta a livello istituzionale. Ci preme prendere nota di quanto si afferma nella relazione di presentazione nella quale si fa riferimento a una “tecnologia che presenta le caratteristiche fortemente invasive della moderna società umana: quella rivolta all’intercettazione acustica e visiva dei nostri movimenti, dei nostri spostamenti, dei nostri incontri quotidiani, a volte dei nostri gesti o atteggiamenti inconsapevoli ma implacabilmente colti da una telecamera ben dissimulata.” I rischi per la privacy sottolineati nella presentazione riguardano gli spazi fisici e quelli morali. Mentre i primi rientrano nel controllo dei movimenti e quindi nel rischio di limitazione degli stessi, i secondi sono messi in rilievo dal riferimento ai “nostri incontri quotidiani” i quali, rientrando nel campo visivo degli occhi elettronici, potrebbero portare a casi di discriminazione sociale. Viene sottolineata inoltre l’urgenza di una normativa in materia ricordando che, in attesa di leggi specifiche, è d’obbligo rifarsi alla legge 675/96 che impone le seguenti misure: informare il Garante nel caso venga predisposto un nuovo sistema di videosorveglianza, informare i cittadini, predisporre un regolamento in caso di registrazione che limiti la conservazione dei nastri adeguandosi alle normative europee già in vigore in paesi quali la Germania, la Spagna e la Francia che hanno fissato i limiti di conservazione a un mese, individuare i pochi fiduciari che possono avere accesso ai filmati.

I dispositivi di videosorveglianza sono indicati come estremamente delicati perché “toccano al cuore la tensione in atto tra Sicurezza, da un lato, e Privatezza, che preferiamo qui utilizzare in luogo di “privacy” a denotare la valenza aperta verso la collettività e la sensibilità pubblica al problema”. Fin dall’inizio si è quindi posto il problema di trovare un equilibrio tra questi due poli nella difficile situazione di rispondere alla domanda di sicurezza da parte dei cittadini pur senza entrare indebitamente nel loro spazio privato. L’indagine svolta ha messo in risalto una totale mancanza di regole riguardo all’installazione dei mezzi presi in esame, sia per quanto riguarda la quantità di telecamere che si possono installare, sia per i casi in cui la presenza delle stesse è giustificata. Anche la necessità di rendere noto ai cittadini la presenza di uno o più impianti di videosorveglianza non sembrava rispondere a una logica unitaria.

I risultati dell’indagine, insieme alla constatazione che le telecamere erano un fenomeno in continua crescita, hanno probabilmente influito sulla decisione del Garante di approvare a fine anno il cosiddetto “decalogo” (<http://www.garanteprivacy.it/garante/doc.jsp?ID=31019>), ovvero i dieci punti che devono essere rispettati per non violare la privacy dei cittadini nel caso si voglia fare uso della videosorveglianza. Il decalogo si rivolge a tutti quei dispositivi che, per fini di sicurezza, permettono la registrazione di immagini. Analizzando le regole fissate nel decalogo è possibile individuare due aree di interesse:

- 1) le *finalità* della videosorveglianza nonché gli scopi per i quali vengono raccolti e in seguito trattati i dati. Per quanto concerne la raccolta, si ribadiscono i concetti già individuati nella comunicazione del febbraio del 2000, ovvero di registrare solo quando è necessario e di evitare immagini dettagliate o ingrandite;
- 2) gli “*osservati*”, ai quali viene ribadito il diritto di essere informati della presenza delle telecamere e dei diritti che possono esercitare.

Nel decalogo si invita inoltre a stabilire con esattezza il limite di tempo inerente all'archiviazione delle immagini e alle persone che possono utilizzare gli impianti. Il principio di finalità e di autodeterminazione informativa sembrano essere le due colonne portanti della prime regole in materia. Il confine tra sicurezza pubblica e privacy dei cittadini è sottolineato nell'*effettiva necessità* di utilizzare tali sistemi: gli scopi, si legge, devono essere legittimi. Se non sussiste una motivazione valida, non è dunque possibile monitorare i cittadini tramite le telecamere. Il rischio di violare l'integrità del corpo è poi chiaramente espresso nella regola numero 6 che invita a limitare l'angolo delle riprese e a non utilizzare senza uno scopo gli zoom. Viene quindi data dignità al “corpo elettronico” sul quale ci siamo soffermati precedentemente. Isolare un “pezzo” del corpo senza un'*effettiva necessità* è ritenuto illecito. Sembra vengano riconosciuti i diritti alla cittadinanza elettronica, alla data-immagine di chi può essere legittimamente controllato senza eccessive ingerenze nello sfera personale.

Nel periodo immediatamente successivo all'approvazione del decalogo, vengono effettuati diversi accertamenti per verificare che le installazioni di telecamere in luoghi pubblici rispettino le regole sopra descritte. I primi interventi dell'Autorità riguardano la mancata segnalazione della videosorveglianza nei pressi degli esercizi commerciali. Sanzioni di questo tipo, ovvero riguardanti la mancata informativa ai cittadini o ai clienti, sembrano essere quelle più numerose. Accanto a problematiche di questo genere, si sono verificati anche casi più gravi, come quello relativo all'installazione da parte di un comune di alcuni sistemi video per il monitoraggio del traffico. Le immagini erano accessibili a chiunque in tempo reale grazie al collegamento al sito web del comune stesso.

Nella Relazione annuale del 2002 il Garante fa un primo bilancio dell'attività svolta in ambito di videosorveglianza dall'anno in cui è stato approvato il decalogo.

Come abbiamo già messo in luce altrove (link al secondo articolo), le finalità per le quali sono utilizzati gli impianti di videosorveglianza sono molteplici. Si legge nella Relazione che “non tutte queste finalità risultano compatibili con i principi sanciti dalla legge n.675” (2002: 98) ed è stata più volte segnalata la necessità di rispettare il decalogo. Nello stesso anno vengono anche indicate precise modalità (riferimento alla newsletter 9-15 settembre 2002) per quanto concerne l'installazione di videosorveglianza sui trasporti pubblici; si specifica, infatti, che le immagini dovranno essere raccolte e conservate solo per fini di sicurezza, e che le riprese all'interno delle vetture non dovranno essere particolareggiate né nei confronti dei passeggeri né nei confronti delle postazioni di guida degli autisti.

Nel 2003 entra in vigore il Codice in materia di protezione dei dati personali (<http://www.garanteprivacy.it/garante/navig/jsp/index.jsp?folderpath=Normativa%2FItaliana%2FI+Codice+in+materia+di+protezione+dei+dati+personali>): per la prima volta nel panorama internazionale viene riunita in un unico corpo normativo la materia in questione. Ricordiamo brevemente che l'articolo 134 del Codice si riferisce alla videosorveglianza, in particolare al Codice di deontologia e buona condotta. Attraverso l'articolo 134 “il Garante promuove, ai sensi dell'articolo 12, la sottoscrizione di un codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato con strumenti elettronici di rilevamento di immagini, prevedendo specifiche modalità di trattamento e forme semplificate di informativa all'interessato per garantire la liceità e la correttezza anche in riferimento a quanto previsto dall'articolo 11”. In quest'ultimo vengono fissate le modalità del trattamento dei dati, ribadendo che questi ultimi devono essere: trattati in modo lecito,

raccolti per fini determinati e utilizzati per altre operazioni in modo compatibile con tali scopi, esatti ed eventualmente aggiornati, non eccedenti rispetto alle finalità per le quali sono raccolti, e, infine, conservati per un periodo limitato di tempo. L'anno successivo viene approvato il "Provvedimento generale sulla videosorveglianza" (<http://www.garanteprivacy.it/garante/doc.jsp?ID=1003482>), che va ad integrare sia il decalogo del 2000 sia a conformare il trattamento dei dati personali tramite videosorveglianza al Codice. Come si legge nella premessa, il presupposto del provvedimento è riferibile all'articolo 2, comma 1 del Codice nel quale vengono specificate le finalità dello stesso, ovvero garantire che il trattamento dei dati personali "si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali". E' inoltre interessante mettere in rilievo che il delicato confine tra sicurezza e privacy è menzionato dal Garante il quale sostiene che la tutela dei dati personali "non pregiudica l'adozione di misure efficaci per garantire la sicurezza dei cittadini e l'accertamento degli illeciti" né è possibile non tutelare all'interno di una società democratica, "la libertà alla circolazione in luoghi pubblici o aperti al pubblico". La privacy non è considerata in antitesi rispetto alla sicurezza: è possibile garantire entrambe senza dimenticarsi dei diritti fondamentali dell'uomo.

Il provvedimento è basato su 4 principi generali: *liceità, necessità, proporzionalità e finalità*. I principi, in linea con il decalogo e con le normative internazionali, ribadiscono che tale mezzo è utilizzabile *solo se* necessario. Vanno evitati usi "superflui ed eccessivi" in aree non a rischio, così come viene ribadito che la videosorveglianza è utilizzabile solo nel momento in cui altre misure siano state ritenute inadeguate per risolvere il problema in questione. Gli aspetti sociali più rilevanti si possono individuare nella descrizione del principio di proporzionalità, nel quale si legge che le telecamere non possono essere installate per "meri fini di apparenza o di prestigio", né va considerata come la misura "meno complicata e di più rapida attuazione che potrebbe non tener conto dell'impatto sui diritti degli altri cittadini o di abbia diversi legittimi interessi".

Viene inoltre esplicitato che l'installazione di telecamere non funzionanti a fini dimostrativi o preventivi può essere "legittimamente oggetto di contestazione" in quanto può influenzare il comportamento e la libertà di movimento delle persone. La proporzionalità rispetto agli scopi deve in ogni caso limitare la raccolta di immagini dettagliate, la durata della loro conservazione e la creazione di una banca dati e il collegamento con altre tecnologie informatiche. Per quanto concerne la conservazione non può essere superiore alle ventiquattro ore, salvo in casi particolari quali la richiesta da parte dell'autorità giudiziaria o di polizia. I diritti degli individui ripresi sono fatti valere attraverso l'obbligo di un'informativa, sotto forma di cartelli che devono essere posti in prossimità delle telecamere. L'informativa deve essere chiara e ben visibile ma non necessariamente a contatto con le telecamere stesse. Inoltre essi possono accedere ai dati che li riguardano e verificare la logica del trattamento.

Oltre al riferimento a settori specifici<sup>4</sup> – quali ospedali o istituti scolastici – nel provvedimento si rimanda esplicitamente alla videosorveglianza effettuata per funzioni di tipo istituzionale, ricordando che "benché effettuata per la cura di un interesse pubblico", devono essere rispettati i principi sopra ricordati. Non è per esempio legittimo monitorare intere aree cittadine in modo continuativo se non sussiste un'effettiva necessità così come non è possibile installare i dispositivi in questione per motivazioni di poca importanza, come controllare che venga rispettato il divieto di fumo o calpestare le aiuole.

---

<sup>4</sup> Si segnala che è stato recentemente approvato un interessante provvedimento (<http://www.garanteprivacy.it/garante/doc.jsp?ID=1246675>) inerente le rilevazioni delle impronte digitali e delle immagini negli istituti di credito.

Ci sono dei casi in cui la videosorveglianza può essere effettuata senza previo consenso dell'Autorità Garante; tra questi rientra "la videosorveglianza senza registrazione", in particolare quella effettuata *mediante impianti a circuito chiuso* in cui le immagini sono visualizzate in tempo reale o conservate per poche ore. A tal proposito vorremmo ricordare che i dispositivi dei quali ci occuperemo nello studio di caso sono indicati nella letteratura anglosassone come "open-street cctv", dove per cctv si intende "closed circuit television", ovvero a circuito chiuso. Il provvedimento sembra poco chiaro quando si riferisce a questa tipologia di impianti, in quanto l'essere "a circuito chiuso" non garantisce la conservazione per poche ore né la sola visualizzazione in tempo reale, come avremo modo di mostrare più avanti. Non sembra del tutto corretto affiancare, come compare nel provvedimento, la videosorveglianza a circuito chiuso dei negozi a quella indicata nello stesso come cctv. Si tratta di due casi differenti e ci pare che il termine utilizzato non possa comprendere anche quella pubblica nelle strade della città. Sebbene il provvedimento del 2004 non nasca all'interno di un "vuoto istituzionale" ma piuttosto confermi le linee nazionali e internazionali in tema di videosorveglianza, si tratta di una cornice legislativa completa che, come abbiamo avuto modo di far rilevare, non trascurava né il delicato rapporto tra sicurezza e privacy né gli aspetti sociali del mezzo di controllo elettronico.